UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

RAISTLIN BEARDSLEY, on behalf of himself and all others similarly situated, *Plaintiff*, v. WARNER MUSIC GROUP CORP., *Defendant.*	Case No. 1:20-cv-07967 **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Raistlin Beardsley ("Plaintiff"), individually and on behalf of all others similarly situated, upon personal knowledge of facts pertaining to himself and on information and belief as to all other matters, by and through undersigned counsel, hereby bring this Class Action Complaint against defendant Warner Music Group Corp. ("Defendant" or "WMG").

I. NATURE OF THE ACTION

1. Plaintiff brings this class action against Defendant for its failure to exercise reasonable care in securing and safeguarding its customers' personal financial data—including credit and debit card records that include cardholder name, card number, expiration date, and internal verification code ("Private Information" or "PI"). Defendant operates thousands of websites through which its customers purchase music and music-related merchandise. In making purchases on Defendant's website, customers enter their PI.

2. On August 5, 2020, Defendant became aware that between April 25, 2020 and August 5, 2020 an unauthorized third party had potentially gained access to PI that customers had provided to Defendant when making purchases on websites Defendant operates ("Data Breach").

3. On or about September 2, 2020, Defendant disclosed the Data Breach to various state Attorneys General. Around this time, Defendant also mailed a document titled "Notice of Data Breach" ("Notice") to its customers, informing them of the Data Breach.

4. Upon information and belief, Plaintiff's and Class members' PI was stolen by hackers. Plaintiff's and Class members' PI may be used for criminal purposes, such as identity theft and fraudulent purchases, and may be sold by the hackers responsible for the Data Breach to other criminals on the dark web.

5. Defendant's security failures enabled the hackers to execute the Data Breach and steal Plaintiff's and Class members' PI. The Data Breach was caused and enabled by Defendant's violation of its obligations to abide by best practices and industry standards concerning the security of payment systems. Defendant failed to comply with security standards and allowed its customers' PI to be compromised by cutting corners on security measures that could have prevented or mitigated the Data Breach that occurred.

6. Defendant's failures put Plaintiff's and Class members' financial information and interests at serious, immediate, and ongoing risk and, additionally, caused costs and expenses to Plaintiff and Class members associated with time and money spent and the loss of productivity as a result of taking time and incurring costs to address and attempt to ameliorate, mitigate and deal with the actual and future consequences of the Data Breach. Plaintiff's and Class members' actions included, as appropriate, finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposing withdrawal and purchase limits on compromised accounts, initiating and monitoring credit freezes, receiving and attempting to stop unwanted SMS text messages, spam emails and phishing emails, travel time and costs associated with the foregoing, and the stress, nuisance and annoyance of dealing with all issues

resulting from the Data Breach. Plaintiff and Class members face ongoing risks of identity theft and financial crimes due to the Data Breach.

7. Accordingly, Plaintiff, on behalf of himself and other members of the Class, asserts claims for negligence, negligence *per se* , unjust enrichment, and the violation of the New York General Business Law, and seeks injunctive relief, monetary damages, statutory damages, and all other relief as authorized in equity or by law.

II. JURISDICTION AND VENUE

8. The Court has jurisdiction over Plaintiff's claims under 28 U.S.C. § 1332(d)(2) ("CAFA"), because (a) there are 100 or more Class members, (b) at least one Class member is a citizen of a state that is diverse from Defendant's citizenship, and (c) the matter in controversy exceeds $5,000,000, exclusive of interest and costs.

9. The Court has personal jurisdiction over Defendant because its principal place of business is located, and it conducts substantial business, in this District.

10. Venue is proper in this District under 28 U.S.C. § 1391(b)(1) because Defendant maintains its principal place of business in this District and therefore resides in this District pursuant to 28 U.S.C. § 1391(c)(2).

III. PARTIES

Plaintiff

11. Plaintiff Raistlin Beardsley is a resident of Saint Helens, Oregon. On or about July 31, 2020, Plaintiff made online purchases ("Purchases") from www.dead.net, and purchased approximately $66 worth of items from this website with his credit card. In order to complete the purchase, Plaintiff was required to – and did - enter his PI into the website, including his name, email address, telephone number, billing and shipping addresses, payment card type, payment card

number, payment card CVV code, and payment card expiration date. Plaintiff received a confirmation email of his July 31, 2020 purchase directly from Defendant's customer service (dead@wmgcustomerservice.com).

12. Plaintiff received the Notice dated September 3, 2020, by U.S. Postal Service mail on or after September 9, 2020.

13. Plaintiff suffered actual injury in the form of damages to and diminution in the value of his PI, a form of intangible property that he entrusted to Defendant for the purpose of making the Purchases, which was compromised as a result of the Data Breach. Additionally, Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft and misuse posed by his PI being placed in the hands of criminals. In addition, Plaintiff suffered actual damages because of the fact that he spent many hours of his time, during which he could of have been working, that he will never get back addressing the data breach.

14. Upon information and belief, Plaintiff's PI has been made available to unauthorized third parties, including through the dark web, as a result of the Data Breach. After the Purchases, Plaintiff received a notice from Experian, a consumer credit reporting company with which Plaintiff maintains credit monitoring, that certain of his PI was on the dark web. Beginning in September 2020 and continuing through the present, Plaintiff has been receiving at least 5 or more unwanted SMS text messages per day on his smartphone, asking him to purchase music-themed facemasks. Since the Purchases, Plaintiff has also received a large number of spam and phishing emails. Plaintiff, could have been working in earning a living during the time that he was forced to expend dealing with these uninvited and unwanted SMS text messages and emails, suffering additional actual damages.

15. Plaintiff has been forced to take a number of time-consuming and burdensome measures as a result of the Data Breach, all of which affords him actual damages because he could and should have been using this time to work and earn a living. In particular, Plaintiff spent time checking all of his credit reports and spent even more time on the telephone placing a credit freeze on his credit reports to prevent identity theft. Plaintiff must now review his financial accounts more closely than he otherwise would. Plaintiff has had to reset some of his online passwords as a precaution against identity theft and fraudulent purchases using his PI. Plaintiff has also attempted, unsuccessfully, to stop all of the unwanted SMS text messages by calling the numbers that these messages are sent from or otherwise trying to identify their origins and blocking the sources of the SMS text messages he was able to figure out. Plaintiff also spent a substantial amount of time on the telephone with his credit card company going over his monthly charges in light of the Data Breach. On a conservative estimate, Plaintiff has spent more than 10 hours thus far in response to the Data Breach, also including time he has spent reviewing the Notice, reviewing Experian's notification of Plaintiff's PI on the dark web, reviewing and attempting to stop not only unwanted SMS text messages but spam and phishing emails as well. Plaintiff's time and efforts would not be necessary but for Defendant's data security shortfalls and failure to safeguard its customers' PI, which made the Data Breach possible.

16. Plaintiff and the other Class members are also at risk of imminent and impending injury arising from the substantially increased risk of future fraud, identity theft, and misuse posed by their PI being stolen by criminals in the Data Breach and, including, but not limited to, the extent that Plaintiff and other Class members still have the payment cards they used to make purchases on websites operated by Defendant. Plaintiff still has at this time the payment card he used to make the Purchases.

17. Plaintiff has a continuing interest in ensuring that his PI is protected and safeguarded from future breaches.

18. The injuries suffered by Plaintiff and Class members as a direct result of the Data Breach include one or more of the following:

a. unauthorized use of their PI;

b. theft of their personal and financial information;

c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

d. damages arising from the inability to use their PI;

e. Time spent and costs associated with the loss of productivity or the enjoyment of one's life from taking time to address and attempt to ameliorate, mitigate and deal with the actual and future consequences of the Data Breach, and the stress, nuisance and annoyance of dealing with all issues resulting from the Data Breach (which time spent on those activities Plaintiff and Class members could have been working and earning a living, therefore suffering further actual injury);

f. the imminent and impending injury flowing from potential fraud and identity theft posed by their PI being placed in the hands of criminals;

g. damages to and diminution in value of their PI entrusted to Defendant for the sole purpose of purchasing products and services from websites operated by Defendant; and

h. the loss of Plaintiff's and Class members' privacy.

Defendant

19. Defendant WMG is a Delaware corporation with its principal place of business in New York, New York.

20. Defendant is a major player in the music industry. Defendant's investor relations website describes it in the following terms:

> With a legacy extending back over 200 years, Warner Music Group today is home to an unparalleled family of creative artists, songwriters, and companies that are moving culture across the globe. At the core of Warner Music Group's Recorded Music division are four of the most iconic companies in history: Atlantic, Elektra, Parlophone and Warner Records. They are joined by renowned labels such as Asylum, Big Beat, Canvasback, East West, Erato, FFRR, Fueled by Ramen, Nonesuch, Reprise, Rhino, Roadrunner, Sire, Spinnin', Warner Classics and Warner Music Nashville. Warner Chappell Music - which traces its origins back to the founding of Chappell & Company in 1811 - is one of the world's leading music publishers, with a catalog of more than 1.4 million copyrights spanning every musical genre from the standards of the Great American Songbook to the biggest hits of the 21st century.[1]

21. Defendant's market cap, as at the date of filing, is approximately $14.35 billion. Defendant's annual turnover is in the billions of dollars. Defendant's 2019 annual report filed with the SEC states that, in the 2019 fiscal year, Defendant's recorded music business generated $3.480 billion of revenue, and its music publishing business generated $643 million of revenue. Defendant operates through subsidiaries, affiliates and non-affiliated licensees in over 60 countries.

22. Defendant was formerly part of Time Warner and was publicly traded on the New York Stock exchange until 2011, when it announced its privatization and sale to Access Industries. On June 3, 2020, Defendant announced an Initial Public Offering on Nasdaq, again becoming a public company.

[1] "About WMG," Investor Relations, https://investors.wmg.com/ (last visited Sept. 25, 2020).

IV. FACTUAL BACKGROUND

Background

23. Defendant operates thousands of websites through which it markets, and makes available for purchase, music and music-related merchandise. These websites include an e-commerce platform that customers must use to make purchases. Defendant places particular emphasis on the role of the internet and new technology in its business strategy. For example, in its 2019 annual report, "[w]e adapted to streaming faster than other major music entertainment companies and were the first such company to report that streaming was the largest source of our recorded music revenue in 2016. Looking into the future, we believe the universe of opportunities will continue to expand…We believe advancements in technology will continue to drive consumer engagement and shape a growing and vibrant music entertainment ecosystem."

24. In order to make purchases through websites operated by Defendant, customers can either create an account or check out as a guest. Either option requires customers to fill out a form on the website, which asks for at least the following PI: (i) full name; (ii) billing address; (iii) shipping address; (iv) email address; (v) telephone number; (vi) name on the payment card the customer intends to use to pay for purchases through the website; (vii) type of the payment card; (viii) full payment card number; (ix) the expiration date of the payment card; and (x) the security code or CVV code for the payment card.

25. Defendant also has a Privacy Policy, addressing its use of customers' PI, which is accessible on websites Defendant operates. The Privacy Policy states under the heading "**SECURITY**" that Defendant "will use reasonable physical, technical and administrative measures to protect Personal Information under our control." Defendant thereby acknowledged

the importance of protecting its customers PI and promised it would use reasonable measures to ensure this PI was protected. However, as described herein, Defendant failed to do so.

The Data Breach

26. On August 5, 2020, Defendant learned that an unauthorized third party had compromised a number of US-based websites Defendant operates, and that the third party may have acquired copies of customers' PI submitted to those websites between April 25, 2020 and August 5, 2020.

27. On or around September 2, 2020 Defendant began notifying state Attorneys General about the Data Breach, including writing letters disclosing the Data Breach to the Attorneys General of Iowa and New Hampshire.

28. On or around September 3, 2020, almost a month after Defendant learned of the Data Breach, Defendant sent customers the Notice. The Notice described the Data Breach in the following manner:

> **WHAT HAPPENED?**
> On August 5, 2020, we learned that an unauthorized third party had compromised a number of US-based e-commerce websites WMG operates but that are hosted and supported by an external service provider. This allowed the unauthorized third party to potentially acquire a copy of the personal information you entered into one or more of the affected website(s) between April 25, 2020 and August 5, 2020. While we cannot definitively confirm that your personal information was affected, it is possible that it might have been as your transaction(s) occurred during the period of compromise. If it was, this might have exposed you to a risk of fraudulent transactions being carried out using your details.
>
> **WHAT INFORMATION WAS INVOLVED?**
> Any personal information you entered into one or more of the affected website(s) between April 25, 2020 and August 5, 2020 after placing an item in your shopping cart was potentially acquired by the unauthorized third party. This could have included your name, email address, telephone number, billing address, shipping address, and payment card details (card number, CVC/CVV and expiration date).
>
> Payments made through PayPal were not affected by this incident.

29. On around September 3, 2020, Defendant filed the Notice with the California Attorney General's Office.

30. As is clear from the Notice and the letters Defendant wrote to state Attorneys General, Defendant failed to detect the Data Breach for over three months, between April 25, 2020 and August 5, 2020. Despite Defendant's promise to its customers that it would use "reasonable physical, technical and administrative measures to protect Personal Information," it failed to do so, and unauthorized individuals were able to illegally access the PI customers had entrusted to Defendant. Further, Defendant waited almost a month before notifying state Attorneys General and its customers of the Data Breach.

31. Defendant claims in the Notice that it "launched a thorough forensic investigation" into the Data Breach and "took steps to address and correct the issue," and that it would offer those impacted 12 months of free identity monitoring services through Kroll. However, all of these steps, including providing identity protection services, are simply reactionary, and do nothing to prevent fraud in the first place nor do they compensate the victims of such fraud. As reported on *Krebs*, a leading security website:[2]

> [Credit monitoring services] are basically PR vehicles for most of the breached companies who offer credit report monitoring to potentially compromised consumers… it does absolutely nothing to compensate for the fact that a criminal stole credit card mag stripe account data… [Credit monitoring services] only give consumers limited help with a very small percentage of the crimes that can be inflicted on them… [a]nd consumers can get most of that limited help for free via the government website or free monitoring from a breached entity where their data inevitably was compromised.

[2] Brian Krebs, *Are Credit Monitoring Services Worth It*, KrebsonSecurity, (Mar. 19, 2014), https://krebsonsecurity.com/2014/03/are-credit-monitoring-services-worth-it/comment-page-1/ (last visited Sept. 25, 2020).

32. Similarly, the ability of credit monitoring services to address issues caused by security breaches like the Data Breach is limited. As recent article on *NerdWallet* commented:[3]

> Credit monitoring services often market themselves as safeguards of your credit profile. But that's not quite the case.
>
> Here's what even the best credit monitoring companies can't do:
>
> - They can't prevent identity theft or credit card fraud.
> - They can't keep you from receiving phishing emails — or from opening them.
> - They can't keep someone from applying for credit in your name.
> - They won't correct errors on your credit report.
> - They won't stop taxpayer identity theft.

33. Reasonable consumers, however, still might resort to obtaining credit monitoring protection because it is almost always advised by the breached merchant, as was the case with Defendant, it is offered by reputable companies, and purports to provide security and monitoring service of value to consumers.

Defendant's Data Security Standards were Inadequate

34. Defendant was on notice of the very real risks of security breaches like the Data Breach. In fact, the Data Breach was not Defendant's first experience of security breaches. Three years ago, Defendant was involved in a phishing scam that caused 3.12 TB of data relating to one of Defendant's music video providers to be leaked.[4]

35. In addition, security breaches like the Data Breach have been frequent and garnered significant media attention over the last decade, with significant data breaches dating back to

[3] Bev O' Shea, "*Credit Monitoring Services: Are They Worth the Cost?*, NerdWallet, (Sept. 21, 2020), https://www.nerdwallet.com/article/finance/credit-monitoring-identity-theft-monitoring (last visited Sept. 25, 2020).

[4] Sarah Coble, *Warner Music Group Discloses Data Breach*, infosecurity (Sept. 4, 2020), https://www.infosecurity-magazine.com/news/warner-music-group-discloses-data/#:~:text=Warner%20Music%20Group%20has%20issued,conglomerate%20on%20August%205%2C%202020 (last visited Sept. 25, 2020).

2005. The Privacy Rights Clearinghouse, a nonprofit organization which focuses on strengthening privacy protections, has recorded over 9,000 data-related security breaches in the U.S. since 2005, including numerous instances of hacking.[5] Any e-commerce provider – indeed, any business which collects PI – is well aware of the risk of security breaches and the need to ensure a robust system of safeguarding against security breaches.

36. In particular, many online commentators have suggested that the Data Breach appears to be a Magecart attack. "Magecart" refers to a number of groups of hackers who use a certain set of tactics to hack into websites and steal individuals' PI, especially payment card information.[6] Magecart hackers usually insert virtual credit card skimmers or scrapers (known as "formjacking") in web applications (usually the shopping cart) and then scrape payment card information (known to hackers as the "fullz"), including the card number, CVV code and billing address.[7] The "fullz" can then be used to make fraudulent purchases and to be sold on the dark web. Magecart hackers may also steal customers' passwords and login details for their online accounts.[8] Based on the information provided in the Notice, it appears the Data Breach was a Magecart attack, or similar to a Magecart attack.

37. Magecart attacks are not a new phenomenon and have garnered significant publicity in recent years. As at September 2019, Magecart attacks were thought to have compromised at

[5] *Data Breaches*, Privacy Rights Clearinghouse, https://privacyrights.org/data-breaches (last visited Sept. 25, 2020).
[6] Scott Ikeda, *Magecart Attacks Alive and Well as Recent Wave Hits High-End Retailers*, CPO Magazine (Sept. 20, 2019), https://www.cpomagazine.com/cyber-security/magecart-attacks-alive-and-well-as-recent-wave-hits-high-end-retailers/ (last visited Sept 25, 2020).
[7] Tara Seals, *Magecart Hits 80 Major eCommerce Sites in Card-Skimming Bonanza*, threatpost (Aug. 28, 2019), https://threatpost.com/magecart-ecommerce-card-skimming-bonanza/147765/ (last visited Sept. 25, 2020).
[8] Scott Ikeda, *Magecart Attacks Alive and Well as Recent Wave Hits High-End Retailers*, CPO Magazine (Sept. 20, 2019), https://www.cpomagazine.com/cyber-security/magecart-attacks-alive-and-well-as-recent-wave-hits-high-end-retailers/ (last visited Sept 25, 2020).

least 50,000 companies worldwide, including British Airways and Ticketmaster.[9] Defendant should have been well aware of the risk of falling victim to a Data Breach, and should have taken steps to secure against such an attack.

38. The main reasons Magecart attacks occur is because websites are not regularly updated to the latest (and most secure) software and because of failures to obfuscate the JavaScript and HTML codes the websites run, which means hackers can easily read the code on these websites and insert the skimming code which enables them to access data entered into the websites.[10] Defendant should have taken these steps, and frequently monitored its e-commerce platforms for malicious codes, in order to ensure security breaches did not occur. Since the malicious code which was responsible for the Data Breach was in place on Defendant's websites for some three months, it is clear that frequent monitoring of Defendant's e-commerce platforms did not occur. Had Defendant detected the malicious code earlier, it could have limited the scope of the Data Breach and the number of its customers whose PI was compromised.

39. Plaintiff and other Class members relied on Defendant, a major, multi-billion dollar company, to have implemented and maintained systems that would keep their PI safe. Defendant had a duty to keep its customers' PI safe, and even acknowledged this in its Privacy Policy, in which Defendant promised to "use reasonable physical, technical and administrative measures" to ensure the security of PI entrusted to it. As discussed above, Defendant failed to comply with this duty.

Defendant Failed to Comply with Industry Standards

[9] *Id.*
[10] *Id.*

40. Federal and State governments have established security standards and issued recommendations to temper data breaches and the resulting harm to consumers and financial institutions. The Federal Trade Commission ("FTC") has issued numerous guides for businesses, highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[11]

41. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which establishes guidelines for fundamental data security principles and practices for business.[12] The guidelines note businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; keep software updated; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

42. The FTC recommends that businesses limit who can access sensitive data; require complex passwords to be used on networks; use industry-tested methods to ensure security and avoid hacking; monitor for suspicious activity on the network; ensure coding in software used by

[11]Federal Trade Commission *Start With Security*, available at https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited Sept. 25, 2020).

[12] Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Sept. 25, 2020).

the business is secure; test systems for common security vulnerabilities and verify that third-party service providers have implemented reasonable security measures.[13]

43. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

44. In addition, Defendant does not claim that it complies with the Payment Card Industry Data Security Standard (PCI DSS).[14] The PCI DSS, formulated by the PCI Security Standards Council, sets out measures that should be taken to ensure data security in relation to online financial transactions. The PCI DSS is designed to ensure that companies maintain consumer credit and debit card information in a secure environment.

45. The PCI DSS was developed to encourage cardholder data security by setting out minimum requirements for businesses to follow. PCI DSS compliance includes, at a minimum, developing and maintaining a security policy that covers all aspects of the business, installing firewalls to protect data, and encrypting cardholder data that is transmitted over public networks by using regularly updated anti-virus software.[15]

46. Despite Defendant's awareness of its data security obligations and its promises to customers that their personal data would be secured and protected, Defendant's treatment of PI

[13] Federal Trade Commission, *Start With Security*, *supra* note 11.
[14] PCI DSS, available at PCI Security Standards Council, *Document Library*, https://www.pcisecuritystandards.org/document_library (last visited Sept. 25, 2020).
[15] *Id.*

entrusted to it by its customers fell far short of satisfying Defendant's legal duties and obligations, and included violations of the PCI DSS. Defendant failed to ensure that access to its data systems was reasonably safeguarded, failed to follow industry standards for the protection of PI and failed to use proper security systems to detect and deter the type of attack that occurred and is at issue here.

47. As a result of Defendant's failure to adhere to industry and government standards for the security of card data, PI of thousands of Defendant's customers, including Plaintiff and Class members, was compromised.

Security Breaches Lead to Identity Theft

48. According to the U.S. Department of Justice Bureau of Justice Statistics, an estimated 17.6 million people were victims of one or more incidents of identity theft in 2014. Among identity theft victims, existing bank or credit accounts were the most common types of misused information.[16]

49. Similarly, the FTC cautions that identity theft wreaks havoc on consumers' finances, credit history, and reputation and can take time, money, and patience to resolve. Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[17]

[16] *See* DOJ, *Victims of Identity Theft, 2014* at 1 (Nov. 13, 2017), available at https://www.bjs.gov/content/pub/pdf/vit14.pdf (last visited Sept. 25, 2020).

[17] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 C.F.R. § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number[.]" *Id.*

50. PI—which includes Plaintiff's and Class members' names combined with their payment card information that were stolen in the Data Breach—is a valuable commodity to identity thieves. At all relevant times, Defendant was well-aware, or reasonably should have been aware, that the PI disclosed by customers on the websites Defendant operates is highly sensitive and could be used for wrongful purposes by third parties, such as identity theft and fraud.

51. Stolen PI is a valuable commodity. A "cyber black-market" on the dark web exists, in which criminals openly post stolen payment card numbers, social security numbers, and other personal information on a number of underground Internet websites. Identity thieves use stolen PI to open new financial accounts and take out loans in another person's name, incur charges on existing accounts, or clone ATM, debit, or credit cards. Stolen PI may be traded on the dark web for years.

52. The growing sophistication of hackers to commit identity theft and fraud are of serious concern and directly implicated in the Data Breach. Hackers are able to gain access to a wide variety of an individual's personal accounts through minimal information.[18] For example, "a billing address and the last four digits of a credit card number are the only two pieces of information anyone needs to get into your iCloud account."[19] From there, "hackers were able to […] take over all of [an individual's] digital devices – and data."[20] Further, hackers have the capability to generate a CVV code "starting with no details at all other than the first six digits" of

[18] Mat Honan, *How Apple and Amazon Security Flaws Led to My Epic Hacking*, (August 6, 2012) https://www.wired.com/2012/08/apple-amazon-mat-honan-hacking/ (last visited September 25, 2020).
[19] *Id.*
[20] *Id.*

a payment card, thereby enabling "hackers [to] obtain the three essential pieces of information to make an online purchase within as little as six seconds."[21]

53. The National Institute of Standards and Technology categorizes the combination of names and credit card numbers as sensitive and warranting a higher impact level based on the potential harm when used in contexts other than their intended use.[22] PI that is "linked" or "linkable" is also more sensitive. Linked information is information about or related to an individual that is logically associated with other information about the individual. Linkable information is information about or related to an individual for which there is a possibility of logical association with other information about the individual. An example of linking information the NIST report cites is a Massachusetts Institute of Technology study showing that 97% of the names and addresses on a voting list were identifiable using only ZIP code and date of birth.

54. PI is broader in scope than directly identifiable information. As technology advances, computer programs become increasingly able to scan the Internet with wider scope to create a mosaic of information that may be used to link information to an individual in ways that were not previously possible.

The Monetary Value of Privacy Protections and Private Information

[21] Newcastle University, *Six Seconds to Hack a Credit Card* (Dec. 2, 2016) https://www.ncl.ac.uk/press/articles/archive/2016/12/cyberattack/ (last visited September 25, 2020).

[22] Erika McCallister, *et al.*, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, National Institute of Standards and Technology Special Publication 800-122, 3-3, available at https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=904990 (last visited Sept. 25, 2020).

55. The fact that Plaintiff's and Class members' PI was stolen, likely in order to be sold on the dark web and/or used for fraudulent transactions, demonstrates the monetary value of the Private Information.

56. At an FTC public workshop in 2001, then-Commissioner Orson Swindle described the value of a consumer's personal information:

> The use of third party information from public records, information aggregators and even competitors for marketing has become a major facilitator of our retail economy. Even [Federal Reserve] Chairman [Alan] Greenspan suggested here some time ago that it's something on the order of the life blood, the free flow of information.[23]

57. Commissioner Swindle's 2001 remarks are even more relevant today, as consumers' personal data functions as a "new form of currency" that supports a $26 billion per year online advertising industry in the United States.[24]

58. The FTC has also recognized that consumer data is a new (and valuable) form of currency. In an FTC roundtable presentation, another former Commissioner, Pamela Jones Harbour, underscored this point:

> Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis—and profit.[25]

---

[23] Tr. at 8:2-8, Federal Trade Commission, *Public Workshop: The Information Marketplace: Merging and Exchanging Consumer Data* (Mar. 13, 2001) available at https://www.ftc.gov/sites/default/files/documents/public_events/information-marketplace-merging-and-exchanging-consumer-data/transcript.pdf (last visited Sept. 25, 2020).

[24] *See* Julia Angwin & Emily Steel, *Web's Hot New Commodity: Privacy*, The Wall Street Journal (Feb. 28, 2011), http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html (last visited Sept. 25, 2020).

[25] *Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable*, (Dec. 7, 2009), https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf (last visited Sept. 25, 2020).

59. Recognizing the high value that consumers place on their PI, many companies now offer consumers an opportunity to sell this information.[26] The idea is to give consumers more power and control over the type of information that they share and who ultimately receives that information. And, by making the transaction transparent, consumers will make a profit from their PI. This business has created a new market for the sale and purchase of this valuable data.

60. Consumers place a high value not only on their PI, but also on the privacy of that data. Researchers have begun to shed light on how much consumers value their data privacy, and the amount is considerable. Indeed, studies confirm that the average direct financial loss for victims of identity theft in 2014 was $1,349.[27]

61. The value of Plaintiff's and Class members' PI on the black market is substantial, ranging from $1.50 to $90 per card number.[28]

62. Despite being aware of the value criminals attach to such PI, and despite its status as a multibillion dollar company which could afford to invest in top-of-the-line data security measures, Defendant failed to ensure its customers were protected from the theft of their PI.

63. At all relevant times, Defendant was well-aware, or reasonably should have been aware, that the PI it maintains is highly sensitive and could be used for wrongful purposes by third parties, such as identity theft and fraud.

---

[26] *See* Julia Angwin & Emily Steel, *Web's Hot New Commodity: Privacy*, The Wall Street Journal (Feb. 28, 2011), http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html (last visited Sept. 25, 2020).

[27] *See* DOJ, *Victims of Identity Theft, 2014* at 1 (Nov. 13, 2017), available at https://www.bjs.gov/content/pub/pdf/vit14.pdf (last visited Sept. 25, 2020), at 6.

[28] Leapfrog, *The Cyber Black Market: What's Your Bank Login Worth* (Mar. 1, 2011), available at https://leapfrogservices.com/the-cyber-black-market-whats-your-bank-login-worth/ (last visited Sept. 25, 2020).

64. Had Defendant remedied the deficiencies in its e-Commerce systems, adequately monitored its e-commerce systems for malicious codes, followed PCI DSS guidelines and, in general, taken reasonable care to prevent and detect security breaches, the Data Breach would have been prevented.

65. Given these facts, any company that transacts business with consumers – who expect their PI to be properly safeguarded - and then compromises the privacy of consumers' PI has thus deprived consumers of the full monetary value of their transaction with the company.

Damages Sustained by Plaintiff and Class Members

66. A portion of the services purchased from Defendant by Plaintiff and the other Class members necessarily included compliance with industry-standard measures with respect to the collection and safeguarding of PI, including their credit and debit card information. The cost to Defendant of collecting and safeguarding PI is built into the price of all its services. Because Plaintiff and the other Class members were denied privacy protections that they paid for and were entitled to receive, Plaintiff and the other Class members incurred actual monetary damages in that they overpaid for the purchases they made through websites operated by Defendant.

67. Plaintiff and the other members of the Class have suffered additional injury and damages, including, but not limited to one or more of the following:

a. unauthorized use of their PI;

b. theft of their personal and financial information;

c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

d. damages arising from the inability to use their PI;

e. Time spent and costs associated with the loss of productivity or the enjoyment of one's life from taking time to address an attempt to ameliorate, mitigate and deal with the actual and future consequences of the Data Breach, and the stress, nuisance and annoyance of dealing with all issues resulting from the Data Breach (which time spent on those activities Plaintiff and Class members could have been working and earning a living, therefore suffering further actual injury);

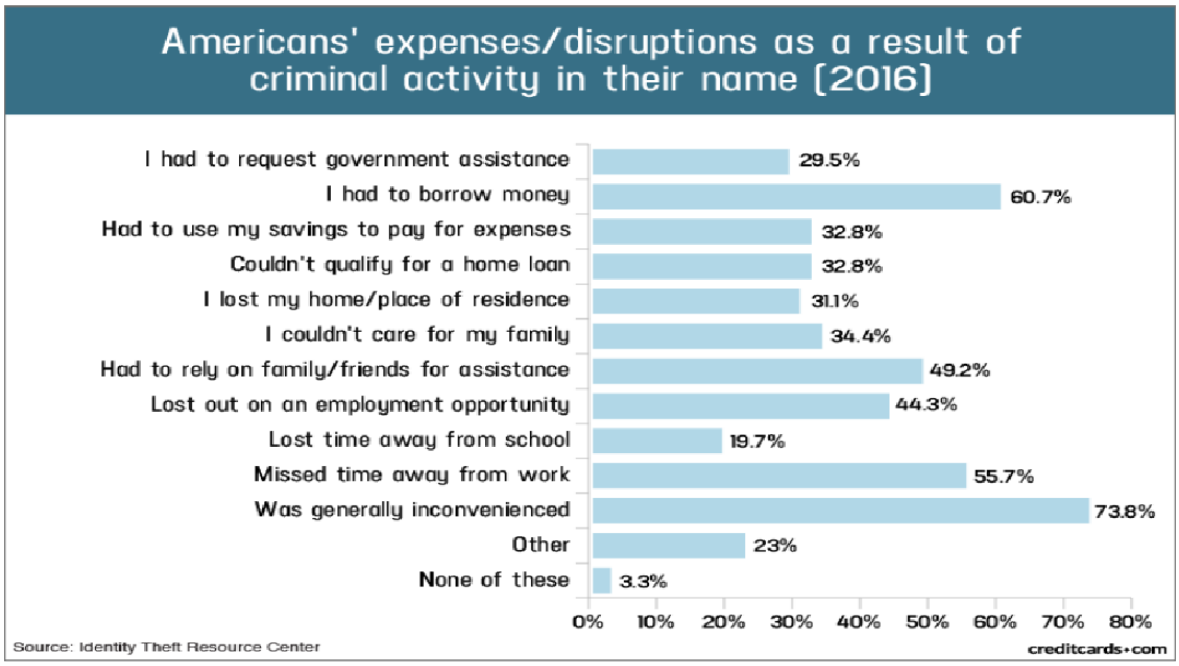
f. the imminent and impending injury flowing from potential fraud and identity theft posed by their PI being placed in the hands of criminals;

g. damages to and diminution in value of their PI entrusted to Defendant for the sole purpose of purchasing products and services from websites operated by Defendant; and

h. the loss of Plaintiff's and Class members' privacy.

68. A study by the Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal information:[29]

[29] Jason Steele, Credit Card and ID Theft Statistics (Oct. 24, 2017) available at https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php (last visited Sept. 25, 2020).



69. Acknowledging the damage to Plaintiff and Class members, Defendant instructed customers who used their payment cards on websites operated by Defendant to take certain cautionary steps. The Notice advised customers "to remain vigilant for any unauthorized use of your payment cards or suspicious email communications." Defendant also advised, in the Notice, that customers should contact their bank or card provider immediately if they noticed suspicious transactions, and provided information from the FTC on how to place a fraud alert or security freeze on their credit file. The burden on Plaintiff and other Class members to deal with the consequences of the Data Breach is obvious from these statements by Defendant.

V. CLASS ACTION ALLEGATIONS

70. Plaintiff brings all counts, as set forth below, on behalf of himself and as a class action, pursuant to the provisions of Rule 23 of the Federal Rules of Civil Procedure, on behalf of a nationwide Class defined as:

> All persons who used their credit, debit, or prepaid debit card on a website operated by Defendant during the period April 25, 2020 to August 5, 2020.

71. Excluded from the Class are Defendant and its affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded is any judicial officer presiding over this matter and the members of their immediate families and judicial staff.

72. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of his claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

73. **Numerosity—Federal Rule of Civil Procedure 23(a)(1).** The members of the Class are so numerous that joinder of all Class members would be impracticable. On information and belief, Class members number in the tens if not hundreds of thousands.

74. **Commonality and Predominance—Federal Rule of Civil Procedure 23(a)(2) and 23(b)(3).** Common questions of law and fact exist as to all Class members and predominate over questions affecting only individual Class members. Such common questions of law or fact include, *inter alia*:

a. Whether Defendant failed to use reasonable care and commercially reasonable methods to secure and safeguard Plaintiff's and Class members' PI;

b. Whether Defendant properly implemented its purported security measures to protect Plaintiff's and Class members' PI from unauthorized capture, dissemination, and misuse;

c. Whether Defendant took reasonable measures to determine the extent of the Data Breach after it first learned of same;

d. Whether Defendant disclosed Plaintiff's and Class members' PI in violation of the understanding that the PI was being disclosed in confidence and should be maintained;

e. Whether Defendant willfully, recklessly, or negligently failed to maintain and execute reasonable procedures designed to prevent unauthorized access to Plaintiff's and Class members' PI;

f. Whether Defendant was negligent in failing to properly secure and protect Plaintiff's and Class members' PI; and

g. Whether Plaintiff and the other members of the Class are entitled to damages, injunctive relief, or other equitable relief, and the measure of such damages and relief.

75. Defendant engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff, on behalf of himself and other Class members. Similar or identical common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that predominate in this action.

76. **Typicality—Federal Rule of Civil Procedure 23(a)(3).** Plaintiff's claims are typical of the claims of the other Class members because, among other things, all Class members were similarly injured through Defendant's uniform misconduct described above and were thus all subject to the Data Breach alleged herein. Further, there are no defenses available to Defendant that are unique to Plaintiff.

77. **Adequacy of Representation—Federal Rule of Civil Procedure 23(a)(4).** Plaintiff is an adequate Class representative because his interests do not conflict with the interests of the other Class members he seeks to represent, he has retained counsel competent and experienced in complex class action litigation, and Plaintiff will prosecute this action vigorously. The Class' interests will be fairly and adequately protected by Plaintiff and his counsel.

78. **Injunctive Relief-Federal Rule of Civil Procedure 23(b)(2).** Defendant has acted and/or refused to act on grounds that apply generally to the Class, making injunctive and/or declaratory relief appropriate with respect to the Class under Fed. Civ. P. 23(b)(2).

79. **Superiority—Federal Rule of Civil Procedure 23(b)(3).** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiff and the other Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendant, so it would be impracticable for Class members to individually seek redress for Defendant's wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

VI. CAUSES OF ACTION

COUNT I
Negligence
(On Behalf of Plaintiff and the Class)

80. Plaintiff, individually and on behalf of the Class, repeats and re-alleges the allegations contained in paragraphs 1 through 79 as though fully set forth herein.

81. Upon accepting and storing Plaintiff's and Class members' PI in its computer systems and on its networks, Defendant undertook and owed a duty to Plaintiff and Class members to exercise reasonable care to secure and safeguard that information and to use commercially

reasonable methods to do so. Defendant knew that the PI was private and confidential and should be protected as private and confidential.

82. Defendant owed a duty of care not to subject Plaintiff's and Class members' PI to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

83. Defendant owed numerous duties to Plaintiff and Class members, including the following:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting PI in its possession;

b. to protect PI using reasonable and adequate security procedures and systems that are compliant with industry-standard practices; and

c. to implement processes to quickly detect a data breach and to timely act on warnings about data breaches.

84. Defendant also breached its duty to Plaintiff and Class members to adequately protect and safeguard PI by knowingly disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured PI. Furthering its dilatory practices, Defendant failed to provide adequate supervision and oversight of the PI with which it was, and is, entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted a malicious third party to gather Plaintiff's and Class members' PI, misuse the PI and intentionally disclose it to others without consent. Defendant further failed to identify the Data Breach for over three months.

85. Defendant knew, or should have known, of the risks inherent in collecting and storing PI, the vulnerabilities of its data collection and/or storage systems, and the importance of adequate security.

86. Defendant knew, or should have known, that its data collection and/or storage systems and networks did not adequately safeguard Plaintiff's and Class members' PI.

87. Defendant breached its duties to Plaintiff and Class members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class members' PI.

88. Because Defendant knew that a breach of its systems would damage an untold number of its customers, including Plaintiff and Class members, Defendant had a duty to adequately protect its data systems and the PI contained thereon.

89. Defendant had a special relationship with Plaintiff and Class members. Plaintiff's and Class members' willingness to entrust Defendant with their PI was predicated on the understanding that Defendant would take adequate security precautions. Moreover, only Defendant had the ability to protect its systems, and the PI it stored on them, from attack.

90. Defendant's own conduct also created a foreseeable risk of harm to Plaintiff and Class members and their PI. Upon information and belief, Defendant's misconduct included failing to: (1) secure its data collection and/or storage systems, despite knowing their vulnerabilities; (2) comply with industry standard security practices; (3) implement adequate system and event monitoring as demonstrated by the span of the Data Breach over several months; and (4) implement the systems, policies, and procedures necessary to prevent this type of data breach.

91. Defendant also had independent duties under state and federal laws that required it to reasonably safeguard Plaintiff's and Class members' PI and promptly notify them about the Data Breach.

92. Defendant breached its duties to Plaintiff and Class members in numerous ways, including:

a. by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class members' PI;
b. by creating a foreseeable risk of harm through the misconduct previously described;
c. by failing to implement adequate security systems, protocols and practices sufficient to protect Plaintiff's and Class members' PI both before and after learning of the Data Breach;
d. by failing to comply with the minimum industry data security standards during the period of the Data Breach; and
e. by failing to timely disclose that Plaintiff's and Class members' PI had been improperly acquired or accessed.

93. Through Defendant's acts and omissions described in this Complaint, including its failure to provide adequate security and its failure to protect Plaintiff's and Class members' PI from being foreseeably captured, accessed, disseminated, stolen and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure Plaintiff's and Class members' PI during the time it was within Defendant's possession or control.

94. The law further imposes an affirmative duty on Defendant to timely disclose the unauthorized access and theft of the PI to Plaintiff and the Class members so that they can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their PI. Defendant failed to do so, only disclosing the Data Breach almost a month after it was detected.

95. Defendant further breached its statutory duties designed to protect the public from harms caused by data breaches, including but not limited to duties to use reasonable measures to protect PI imposed by Section 5 of the Federal Trade Commission Act (the "FTCA").

96. Through Defendant's acts and omissions described in this Complaint, including Defendant's failure to provide adequate security and their failure to protect Plaintiff's and Class members' PI from being foreseeably captured, accessed, disseminated, stolen and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure Plaintiff's and Class members' PI during the time it was within Defendant's possession or control.

97. Further, through their failure to discover the Data Breach for a period exceeding three months, Defendant prevented Plaintiff and Class members from taking meaningful, proactive steps to secure their financial data and bank accounts.

98. Upon information and belief, Defendant improperly and inadequately safeguarded Plaintiff's and Class members' PI in deviation of standard industry rules, regulations, and practices at the time of the unauthorized access. Defendant's failure to take proper security measures to protect Plaintiff's and Class members' sensitive PI, as described in this Complaint, created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access of the PI.

99. Upon information and belief, neither Plaintiff nor the other Class members contributed to the Data Breach and subsequent misuse of their PI as described in this Complaint.

100. As a direct and proximate cause of Defendant's conduct, Plaintiff and Class members suffered Plaintiff and Class members have suffered and will suffer damages and injury, including but not limited to:

a. unauthorized use of their PI;

b. theft of their personal and financial information;

c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

d. damages arising from the inability to use their PI;

e. Time spent and costs associated with the loss of productivity or the enjoyment of one's life from taking time to address and attempt to ameliorate, mitigate and deal with the actual and future consequences of the Data Breach, and the stress, nuisance and annoyance of dealing with all issues resulting from the Data Breach (which time spent on those activities Plaintiff and Class members could have been working and earning a living, therefore suffering further actual injury);

f. the imminent and impending injury flowing from potential fraud and identity theft posed by their PI being placed in the hands of criminals;

g. damages to and diminution in value of their PI entrusted to Defendant for the sole purpose of purchasing products and services from websites operated by Defendant; and

h. the loss of Plaintiff's and Class members' privacy.

101. As a direct and proximate cause of Defendant's negligence, Plaintiff and Class members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

COUNT II
Negligence *Per Se*

(On Behalf of Plaintiff and the Class)

102. Plaintiff, individually and on behalf of the Class, repeats and re-alleges the allegations contained in paragraphs 1 through 79 as though fully set forth herein.

103. Section 5 of the FTCA bars unfair and deceptive acts and practices "in or affecting commerce," which the FTC has interpreted and enforced as including action against organizations that have violated consumers' privacy rights and/or misled consumers through a failure to maintain appropriate security for sensitive information, such as the PI of Plaintiff and Class members. The FTC guidance discussed above also serves to further the Defendant's duty to Plaintiff and Class members.

104. Defendant violated Section 5 of the FTCA in its failure to implement reasonable safeguards to protect the PI of Plaintiff and Class members and in its abandonment of industry standards regarding the protection of consumers' PI. Defendant's violation of Section 5 of the FTCA is all the more unreasonable in light of the vast size of Defendant's consumer base, as well as the particularly sensitive nature of Plaintiff's and Class members' PI that was collected and stored.

105. Defendant's violation of Section 5 of the FTCA is negligence *per se*.

106. Plaintiff and Class members are within the class of persons that the FTCA intends to protect.

107. The harm sustained by Plaintiff and Class members as a result of the Data Breach is the type of harm that the FTCA was intended to safeguard the public against. The FTC has taken enforcement action against organizations failing to implement reasonable and proper measures to protect consumers' sensitive data, as these acts constitute unfair and deceptive practices. These harms are the same as those suffered by Plaintiff and Class members in this action.

108. As a direct and proximate cause of Defendant's negligence *per se*, Plaintiff and Class members have suffered and will suffer injury, including but not limited to:

a. unauthorized use of their PI;

b. theft of their personal and financial information;

c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

d. damages arising from the inability to use their PI;

e. Time spent and costs associated with the loss of productivity or the enjoyment of one's life from taking time to address and attempt to ameliorate, mitigate and deal with the actual and future consequences of the Data Breach, and the stress, nuisance and annoyance of dealing with all issues resulting from the Data Breach (which time spent on those activities Plaintiff and Class members could have been working and earning a living, therefore suffering further actual injury);

f. the imminent and impending injury flowing from potential fraud and identity theft posed by their PI being placed in the hands of criminals;

g. damages to and diminution in value of their PI entrusted to Defendant for the sole purpose of purchasing products and services from websites operated by Defendant; and

h. the loss of Plaintiff's and Class members' privacy.

109. As a direct and proximate cause of Defendant's negligence *per se*, Plaintiff and Class members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

COUNT III
Violations of New York Consumer Law for Deceptive Acts and Practices
N.Y. Gen. Bus. Law § 349
(On Behalf of Plaintiff and the Class)

110. Plaintiff, individually and on behalf of the Class, repeats and re-alleges the allegations contained in paragraphs 1 through 79 as though fully set forth herein.

111. New York General Business Law ("NYGBL") § 349 prohibits deceptive acts or practices in the conduct of any business, trade, or commerce, or in the furnishing of any service in the state of New York.

112. The law of the State of New York applies to all customer disputes with respect to customer purchases from Defendant's e-commerce websites.

113. By reason of the conduct alleged herein, Defendant engaged in unlawful practices within the meaning of the NYGBL § 349. The conduct alleged herein is a "business practice" within the meaning of the NYGBL § 349, and the deception occurred in part within New York State.

114. Defendant stored Plaintiff's and the Class members' PI in Defendant's electronic and consumer information databases. Defendant knew or should have known that it did not employ reasonable, industry standard, and appropriate security measures that complied "with federal regulations" and that would have kept Plaintiff's and the Class members' PI secure and prevented the loss or misuse of Plaintiff's and the Class members' PI. Defendant did not disclose to Plaintiff and the Class members that its data systems were not secure.

115. Plaintiff and the Class members never would have provided their sensitive and personal PI if they had been told or knew that Defendant failed to maintain sufficient security to keep such PI from being hacked and taken by others, and that Defendant failed to maintain the information in a properly encrypted form.

116. Defendant violated the NYGBL §349 by misrepresenting, both by affirmative conduct and by omission, the safety of Defendant's many systems and services, specifically the security thereof, and their ability to safely store Plaintiff's and the Class members' PI.

117. Defendant also violated NYGBL §349 by failing to implement reasonable and appropriate security measures or follow industry standards for data security, and by failing to immediately notify Plaintiff and the Class members of the Data Breach. If Defendant had complied with these legal requirements, Plaintiff and the other Class members would not have suffered the extent of damages caused by the Data Breach.

118. Defendant's practices, acts, policies and course of conduct violate NYGBL § 349 in that:

a. Defendant actively and knowingly misrepresented or omitted disclosure of material information to Plaintiff and the Class members at the time they provided such PI that Defendant did not have sufficient security or mechanisms to protect PI;

b. Defendant failed to give timely warnings and notices regarding the defects and problems with its system(s) of security that it maintained to protect Plaintiff's and the Class members' PI. Upon information and belief, Defendant possessed prior knowledge of the inherent defects in its IT systems and failed to address the same or to give timely warnings that there had been a Data Breach.

119. Plaintiff and Class members were entitled to assume, and did assume, Defendant would take appropriate measures to keep their PI safe. Defendant did not disclose at any time that Plaintiff's and the Class members' PI was vulnerable to hackers because Defendant's data security measures were inadequate, and Defendant was the only one in possession of that material information, which it had a duty to disclose.

120. The aforementioned conduct is and was deceptive, false, and fraudulent and constitutes an unconscionable commercial practice in that Defendant has, by the use of false or deceptive statements and/or knowing intentional material omissions, misrepresented and/or concealed the defective security system it maintained and failed to reveal the Data Breach timely and adequately.

121. Members of the public were deceived by and relied upon Defendant's affirmative misrepresentations and failures to disclose.

122. Such acts by Defendant are and were deceptive acts or practices which are and/or were likely to mislead a reasonable consumer providing his or her PI to Defendant. Said deceptive acts and practices are material. The requests for and use of such PI in New York through deceptive means occurring in New York were consumer-oriented acts and thereby fall under the New York consumer fraud statute, NYGBL § 349.

123. Defendant's wrongful conduct caused Plaintiff and the Class members to suffer a consumer-related injury by causing them to incur actual and future loss of time and expense to protect from misuse of the PI materials by third parties and placing the Plaintiff and the Class members at serious risk for monetary damages.

124. As a direct and proximate cause of Defendant's conduct, Plaintiff and Class members suffered damages as alleged above.

125. In addition to or in lieu of actual damages, because of the injury, Plaintiff and the Class members seek statutory damages for each injury and violation which has occurred.

COUNT IV
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

126. Plaintiff, individually and on behalf of the Class, repeats and re-alleges the allegations contained in paragraphs 1 through 79 as though fully set forth herein.

127. Plaintiff and Class members conferred a monetary benefit on Defendant. Specifically, they purchased goods and services from Defendant and provided Defendant with their payment information. In exchange, Plaintiff and Class members should have received from Defendant the goods and services that were the subject of the transaction with protection of their PI with adequate data security.

128. Defendant knew that Plaintiff and Class members conferred a benefit on them and accepted and has accepted or retained that benefit. Defendant profited from Plaintiff's purchases and used Plaintiff's and Class members' PI for business purposes.

129. Defendant failed to secure Plaintiff's and Class members' PI and, therefore, did not provide full compensation for the benefit the Plaintiff's and Class members' PI provided.

130. Defendant acquired the PI through inequitable means as they failed to disclose the inadequate security practices previously alleged.

131. If Plaintiff and Class members knew that Defendant would not secure their PI using adequate security, they would not have made purchases on Defendant's website.

132. Plaintiff and Class members have no adequate remedy at law.

133. Under the circumstances, it would be unjust for Defendant to be permitted to retain any of the benefits that Plaintiff and Class members conferred on them.

134. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class members, proceeds that they unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and Class members overpaid.

VII. DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury of all claims so triable.

VIII. REQUEST FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the other members of the Class proposed in this Complaint, respectfully requests that the Court enter judgment in his and the Class' favor and against Defendant, as follows:

A. Declaring that this action is a proper class action, certifying the Class as requested herein, designating Plaintiff as Class Representative, and appointing Class Counsel as requested in Plaintiff's expected motion for class certification;

B. Ordering Defendant to pay actual/statutory damages as appropriate to Plaintiff and the other members of the Class;

C. Ordering Defendant to pay punitive damages, as allowable by law, to Plaintiff and the other members of the Class;

D. Ordering Defendant to pay attorneys' fees and litigation costs to Plaintiff and his counsel;

E. Ordering Defendant to pay equitable relief, in the form of disgorgement and restitution, and injunctive relief as may be appropriate;

F. Ordering Defendant to pay both pre- and post-judgment interest on any amounts awarded; and

G. Ordering such other and further relief as may be just and proper.

Date: September 25, 2020.

Respectfully submitted,

/s/ Lori G. Feldman

Lori G. Feldman
GEORGE GESTEN MCDONALD PLLC
102 Half Moon Bay Drive
Croton-on-Hudson, New York 10520
Phone: (917) 983-9321

Fax: (888) 421-4173
Email: LFeldman@4-justice.com
E-Service: eService@4-Justice.com

David J. George
GEORGE GESTEN MCDONALD, PLLC
9897 Lake Worth Road, Suite #302
Lake Worth, FL 33467
Phone: (561) 232-6002
Fax: (888) 421-4173
Email: DGeorge@4-Justice.com
E-Service: eService@4-Justice.com

/s/ Janine L. Pollack
Janine L. Pollack
CALCATERRA POLLACK LLP
1140 Avenue of the Americas
9th Floor
New York, New York 10036
Phone:(212) 899-1760
Email: jpollack@calcaterrapollack.com
JUSTIN TERES
Email: jteres@calcaterrapollack.com